HN

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/809,073	03/16/2001	Lee Codel Lawson Tarbotton	550-221	5551

23117 7590 03/22/2005

NIXON & VANDERHYE, PC
1100 N GLEBE ROAD
8TH FLOOR
ARLINGTON, VA 22201-4714

EXAMINER	
SIMITOSKI, MICHAEL J	
ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 03/22/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/809,073	TARBOTTON ET AL.	
	Examiner	Art Unit	
	Michael J Simitoski	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 December 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,4-8,10-16,18-22,24-30,32-36 and 38-42* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,4-8,10-16,18-22,24-30,32-36 and 38-42* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *21 December 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. The response of 10/27/2004 was received and considered.

2. Claims 1-2, 4-8, 10-16, 18-22, 24-30, 32-36 & 38-42 are pending.

Response to Arguments

3. Applicant's drawings submitted 10/27/2004 are accepted; the objections to the drawings, set forth in the previous Office Action, are withdrawn.

4. The submitted abstract is accepted; the objections are withdrawn.

5. In light of applicant's amendments, the objections to the specification and claims, set forth in the previous Office Action, are withdrawn.

6. In light of Applicant's cancellation of claims 3, 9, 17, 23, 31 & 37, the rejections of those claims under 35 U.S.C. §112, set forth in the previous Office Action, are withdrawn.

7. Applicant's arguments filed 10/27/2004 have been fully considered but they are not persuasive. Further, Applicant's arguments are moot in view of new grounds of rejection.

Applicant's response (p. 20, ¶4) argues that the banned computer programs in the claims are not computer virus programs. The limitation "non-virus" program is indefinite because there is no concrete (standard) difference between a virus program and a non-virus program. Many non-virus programs perform unwanted actions on a computer. Further, as evidenced by the newly cited "Why does NAV indicate a virus alert with the Flash Player?" by Wobensmith, the Symantec product does not necessarily only detect those programs that have been previously established to be viruses. Therefore, the argument that Norton and Hedberg are not material to Applicant's claims is not persuasive.

Applicant's response (p. 21, ¶2 – p. 22, ¶1) argues that no motivation exists to combine the automated mechanisms of Hedberg to the Norton system. The Examiner disagrees. The Hedberg system allows the automated generation of virus definitions, specifically a user doesn't have to specify all the specific details of the signature. Applicant states

> "The Norton system teaches that as soon as a user adds the suspect file to the quarantine list, then that file is encrypted and is no longer available for use at that computer. As a result, after encryption, there is no outstanding problem for the user at that computer because the file has already been dealt with. There would be no reason to add computer virus sighnature generating mechanisms (as allegedly taught by Hedberg) to the computer, since the original computer is already protected from the suspicious file by virtue of the quarantine and encryption of that computer file."

However, Hedberg is cited for teaching that rather than manually write a virus definition file, a mechanism can be used to create one automatically. Symantec lacks creating a virus signature definition, but Hedberg teaches that a software can function to create it's own, without requiring human intervention in the actual creation of the definition files. Further, Applicant reasons that "Even if the automatic virus signature generation mechanism (allegedly taught by Hedberg) were added to the computer, there would be nothing for the mechanism to detect, since the computer file which should be targeted has already been quarantined and subsequently encrypted." However, the reason a virus definition is created for any program is so that any *future* attempts of the virus to enter the system are contained. It is well understood in the art of virus protection that virus signatures are distributed for multiple purposes, mainly to prevent an initial viral infection, to prevent *further* viral infections and to repair virus-damaged files. While the user can specify a piece of software to quarantine in Symantec, the user is expected to send the virus program to experts, who will then create a definition if the software is in fact a virus. What Hedberg teaches is that a program can be made to generate definitions on it's own. One of ordinary skill in the art

would recognize this as beneficial because any future receptions of the same executable would be caught.

Applicant's response (p. 22, ¶2) states one of the benefits of the claimed invention being that the definition files may be distributed to other machines on a network and states that this "beneficial functionality of Applicants' independent claim 1 is neither disclosed nor suggested in any of the prior art references." However, this is not recited in any of the independent claims. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Claim Rejections - 35 USC § 112

8. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

9. Claims 1-2, 4-8, 10-16, 18-22, 24-30, 32-36 & 38-42 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. The banning of an "undesired, non-virus computer program" is not described in the specification.

10. Claims 21-22 & 24-28 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not

described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. Claim 21 presents a single method step, which fails to comply with the enablement requirement, see 2164.08(a).

11. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

12. Claims 1-2 & 4-6 & 21 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Regarding claim 1, the limitation "said computer controlling program comprising" is unclear.

Regarding claims 1, 7, 15, 21, 29 & 35, the limitation "undesired" is indefinite because what is undesired to one person is not necessarily undesired to another.

Regarding claims 1, 7, 15, 21, 29 & 35, the limitation "non-virus" program is indefinite because there is no concrete difference between a virus program and a non-virus program. Many non-virus programs perform unwanted actions on a computer.

Regarding claim 21, it is unclear if the "user generated program identifying data" is a method step.

Regarding claim 22, the step of "operating ... to identify" has no tangible output.

Claim Rejections - 35 USC § 103

13. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

14. Claims 1, 4, 6-7, 11-14, 29, 32 & 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over "Norton AntiVirus User's Guide", by Symantec Corporation (Symantec) in view of "Combating computer viruses: IBM's new computer immune system" by Hedberg.

Regarding claims 1, 4, 6-7, 14, 29, 32 & 34, Symantec discloses a user controlled program identifying data generating logic/Norton AntiVirus to generate banned program identifying data/encrypted suspected virus for said one or more computer programs/suspected viruses to be banned from use/quarantined (page 31, ¶1, page 45, §Submitting files to SARC & page 46). Symantec lacks said banned program identifying data/encrypted suspected virus being operable to control anti computer virus logic to identify computer programs banned from use. However, Hedberg teaches that anti-virus software can be made to detect variations of known viruses and extract identification signatures for them (pages 10-11 & Fig. 1) to eliminate the need for the slower traditional approach (page 10, §A neural network virus classifier). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to create banned program identifying data that is operable to control anti computer virus logic to identify the computer programs/viruses banned from use. One of ordinary skill in the art would have been motivated to perform such a modification to eliminate

the need for the slower (page 10, §A neural network virus classifier) traditional analysis approach, as taught by Hedberg (pages 10-11 & Fig. 1).

Regarding claim 11, Symantec discloses that the program can be encrypted/quarantined or deleted (pages 39-40).

Regarding claim 12, Symantec, as modified above, discloses restoring the banned program identifying data/virus definitions from a remote source/LiveUpdate server (page 18).

Regarding claim 13, Symantec, as modified above, lacks explicit disclosure of the anti computer virus logic being executable as a separate instance solely to identify computer programs banned from use. However, the examiner takes Official Notice that running separate processes on a computer is old and well established in the art of computer application processing as a method of increasing the modularity of software code. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to execute the anti computer virus logic as a separate instance. One of ordinary skill in the art would have been motivated to perform such a modification to allow the use of the software separately from other software components. This advantage is well known to those skilled in the art.

15. Claims 2, 8 & 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Symantec in view of Hedberg, as applied to claim 1 above, in further view of "Bad IDEA" by Peter Szor (Szor), in further view of "Cryptography in Everyday Life" by Sarah Simpson (Simpson). Symantec, as modified above, lacks encrypting the banned program identifying data with a private key. However, Szor teaches that to prevent modification of antivirus signature files, the files should be encrypted (page 19, ¶2). Therefore, it would have been obvious to one

having ordinary skill in the art at the time the invention was made to encrypt the banned program identifying data. One of ordinary skill in the art would have been motivated to perform such a modification to prevent modification of antivirus signature files, as taught by Szor (page 19, ¶2). As modified, Symantec lacks using a PGP private key. However, Simpson teaches that by encrypting a file with a private key, the sender can be verified by decrypting it with the corresponding public key (page 1, ¶1) and that PGP provides such encryption and authentication (page 1, ¶2). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use a PGP private key. One of ordinary skill in the art would have been motivated to perform such a modification to verify the creator of the signature files, as taught by Simpson (page 1).

16. Claims 5 & 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Symantec, in view of Hedberg, as applied to claims 4, 18 & 32 above, in further view of "Heuristic Anti-Virus Technology" by Veldman. Symantec, as modified above, discloses detecting variants of known viruses, but lacks the banned program identifying data including heuristic data identifying one or more behavioral characteristics. However, Veldman teaches that using heuristics and examining behaviors of a program allows detection of unknown viruses (§1 & §2.1). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to including in the identifying data, heuristic data identifying one or more behavioral characteristics. One of ordinary skill in the art would have been motivated to perform such a modification to detect unknown computer viruses, as taught by Veldman (§1, ¶1 & §2.1).

17. Claims 10 & 38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Symantec, in view of Hedberg, Szor & Simpson, as applied to claims 8, 22 & 36, in further view of U.S. Patent 5,844,986 to Davis. Symantec, as modified above, lacks storing the identifying data in a secure memory region. However, Davis teaches that to prevent a virus from corrupting a BIOS (flash memory), an authentication and validation procedure is required before its contents can be modified (col. 1, lines 32-45 & 63-67). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to store the identifying data in a secure memory region (memory requiring authentication). One of ordinary skill in the art would have been motivated to perform such a modification to prevent a virus from corrupting the identifying data, as taught by Davis (col. 1, lines 32-45 & 63-67).

18. Claims 1, 4, 6-7, 11-15, 18, 20-21, 25-29, 32, 34-35 & 39-42 are rejected under 35 U.S.C. 103(a) as being unpatentable over "Norton AntiVirus User's Guide", by Symantec Corporation (Symantec) in view of "Combating computer viruses: IBM's new computer immune system" by Hedberg in further view of "Ad-aware" by Lavasoft.

Regarding claims 1, 4, 6-7, 14-15, 18, 20-21, 28-29, 32, 34-35 & 42, Symantec discloses a user controlled program identifying data generating logic/Norton AntiVirus to generate banned program identifying data/encrypted suspected virus for said one or more computer programs/suspected viruses to be banned from use/quarantined (page 31, ¶1, page 45, §Submitting files to SARC & page 46). Symantec lacks said banned program identifying data/encrypted suspected virus being operable to control anti computer virus logic to identify computer programs banned from use. However, Hedberg teaches that anti-virus software can be

made to detect variations of known viruses and extract identification signatures for them (pages 10-11 & Fig. 1) to eliminate the need for the slower traditional approach (page 10, §A neural network virus classifier). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to create banned program identifying data that is operable to control anti computer virus logic to identify the computer programs/viruses banned from use. One of ordinary skill in the art would have been motivated to perform such a modification to eliminate the need for the slower (page 10, §A neural network virus classifier) traditional analysis approach, as taught by Hedberg (pages 10-11 & Fig. 1). As modified, Symantec does not disclose banning "undesired, non-virus computer program[s]". However, Lavasoft teaches that Ad-aware is a program that removes spyware by scanning "your memory, registry and harddrives for known spyware and lets you remove them safely" (p. 1). Further, Lavasoft teaches "Ad-watch, included in the Ad-aware plus package, is a real-time spyware-monitor, watching your memory and registry for spyware that tries to install or change your system" (p. 1). Ad-aware is essentially a virus-scanner that monitors/scans for and removes non-virus programs. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to ban undesired, non-virus programs/spyware. One of ordinary skill in the art would have been motivated to perform such a modification to safely remove spyware, as taught by Lavasoft (p. 1).

Regarding claims 11, 25 & 39, Symantec discloses that the program can be encrypted/quarantined or deleted (pages 39-40).

Regarding claims 12, 26 & 40, Symantec, as modified above, discloses restoring the banned program identifying data/virus definitions from a remote source/LiveUpdate server (page 18).

Regarding claims 13, 27 & 41, Symantec, as modified above, lacks explicit disclosure of the anti computer virus logic being executable as a separate instance solely to identify computer programs banned from use. However, the examiner takes Official Notice that running separate processes on a computer is old and well established in the art of computer application processing as a method of increasing the modularity of software code. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to execute the anti computer virus logic as a separate instance. One of ordinary skill in the art would have been motivated to perform such a modification to allow the use of the software separately from other software components. This advantage is well known to those skilled in the art.

19. Claims 2, 8, 16, 22, 30 & 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Symantec, Hedberg & Lavasoft, as applied to claim 1 above, in further view of "Bad IDEA" by Peter Szor (Szor), in further view of "Cryptography in Everyday Life" by Sarah Simpson (Simpson). Symantec, as modified above, lacks encrypting the banned program identifying data with a private key. However, Szor teaches that to prevent modification of antivirus signature files, the files should be encrypted (page 19, ¶2). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to encrypt the banned program identifying data. One of ordinary skill in the art would have been motivated to perform such a modification to prevent modification of antivirus signature files, as taught by

Szor (page 19, ¶2). As modified, Symantec lacks using a PGP private key. However, Simpson teaches that by encrypting a file with a private key, the sender can be verified by decrypting it with the corresponding public key (page 1, ¶1) and that PGP provides such encryption and authentication (page 1, ¶2). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use a PGP private key. One of ordinary skill in the art would have been motivated to perform such a modification to verify the creator of the signature files, as taught by Simpson (page 1).

20. Claims 5, 19 & 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Symantec, Hedberg & Lavasoft, as applied to claims 4, 18 & 32 above, in further view of "Heuristic Anti-Virus Technology" by Veldman. Symantec, as modified above, discloses detecting variants of known viruses, but lacks the banned program identifying data including heuristic data identifying one or more behavioral characteristics. However, Veldman teaches that using heuristics and examining behaviors of a program allows detection of unknown viruses (§1 & §2.1). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to including in the identifying data, heuristic data identifying one or more behavioral characteristics. One of ordinary skill in the art would have been motivated to perform such a modification to detect unknown computer viruses, as taught by Veldman (§1, ¶1 & §2.1).

21. Claims 10, 24 & 38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Symantec, Hedberg, Lavasoft, Szor & Simpson, as applied to claims 8, 22 & 36, in further view

of U.S. Patent 5,844,986 to Davis. Symantec, as modified above, lacks storing the identifying data in a secure memory region. However, Davis teaches that to prevent a virus from corrupting a BIOS (flash memory), an authentication and validation procedure is required before its contents can be modified (col. 1, lines 32-45 & 63-67). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to store the identifying data in a secure memory region (memory requiring authentication). One of ordinary skill in the art would have been motivated to perform such a modification to prevent a virus from corrupting the identifying data, as taught by Davis (col. 1, lines 32-45 & 63-67).

Conclusion

22. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

23. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (571) 272-3841. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m.. The examiner can also be reached on alternate Fridays from 6:45 a.m. – 3:15 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached at (571) 272-3838.

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks
Washington, DC 20231

Or faxed to:

(703)746-7239 (for formal communications intended for entry)

Or:

(571)273-3841 (Examiner's fax, for informal or draft communications, please label "PROPOSED" or "DRAFT")

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2100.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MJS
March 7, 2005

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100